Proceedings of the International Conference , "Computational Systems for Health & Sustainability"
17-18, April, 2015 - by R.V.College of Engineering,
Bangalore,Karnataka,PIN-560059,INDIA

IDENTITY PRIVACY AND PRESERVING DATA IN MULTI-ATTORNEY MANNER USING CLOUD

Vijaya kumar patil C
Dept. Of Computer Science & Engg.
Mangalore Institute of Technology and Engineering
Mangalore, Karnataka, India

Manjunath H
HOD, Dept.Of Information Science & Engg.
Mangalore Institute of Technology and Engineering
Mangalore, Karnataka, India

ABSTRACT: Cloud computing provides an economical and efficient solution for sharing data among the cloud users in the group , users sharing data in a multi-attorney manner preserving data and identity privacy from an untrusted cloud, it is still a challenging issue, due to frequent change of the membership in the group. In this paper, we propose a multi-attorney data sharing scheme for the dynamic groups in the cloud. By combing group signature and dynamic broadcast encryption techniques, any cloud user anonymously share the data with others. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

Index terms-cloud computing, data sharing, privacy-preserving, access control, and dynamic groups**.**

1. INTODUCTION

Cloud computing is recognized as an alternative to traditional information technology [1] due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve dataprivacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [2]. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following

Challengingissues:

First, identity privacy is one of the most significantobstacles for the wide deployment of cloud computing.Without the guarantee of identity privacy, users may beunwilling to join in cloud computing systems because their real identities

could be easily disclosed to cloud providers and attackers. On the Other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable.

Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multi-attorney manner. Compared with the single-attorney manner [3], where only the group manager can store and modify data in the cloud, the multiple-attorney manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/ her part of data in the entire data file shared by the company.

Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employeerevocation in a company. The changes of membership makesecure data sharing extremely difficult. On one hand, theanonymous system challenges new granted users to learnthe content of data files stored before their participation,because it is impossible for new granted users to contactwith anonymous data owners, and obtain the correspondingdecryption keys. On the other hand, an efficientmembership revocation mechanism without updating thesecret keys of the remaining users is also desired tominimize the complexity of key management. Several security schemes for data sharing on untrusted servers have been proposed [4], [5], [6]. In these approaches,data owners store the encrypted data files in untrustedstorage and distribute the corresponding decryption keysonly to authorized users. Thus, unauthorized users as wellas storage servers cannot learn the content of the data filesbecause they have no knowledge of the decryption keys However, the complexities of user participation and revocationin these schemes are linearly increasing with thenumber of data owners and the number of revoked users,respectively. By setting a group with a single attribute, Lu etal. [7] proposed a secure provenance scheme based on thecipher text-policy attribute-based encryption technique [8],which allows any member in a group to share data withothers. However, the issue of user revocation

is notaddressed in their scheme. Yu et al. [3] presented a scalableand fine-grained data access control scheme in cloudcomputing based on the key policy attribute-based encryption(KP-ABE) technique [9]. Unfortunately, the single-attorney manner hinders the adoption of their scheme into thecase, where any user is granted to store and share data.Our contributions. To solve the challenges presentedabove, we propose Mona, a secure multi-attorney datasharing scheme for dynamic groups in the cloud. The maincontributions of this paper include:

1. We propose a secure multi-attorney data sharingscheme. It implies that any user in the group cansecurely share data with others by the untrustedcloud.

2. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners.User revocation can be easily achieved through anovel revocation list without updating the secretkeys of the remaining users. The size and computationoverhead of encryption are constant andindependent with the number of revoked users.

3. We provide secure and privacy-preserving accesscontrol to users, which guarantees any member in agroup to anonymously utilize the cloud resource.Moreover, the real identities of data owners can berevealed by the group manager when disputes occur.

4. We provide rigorous security analysis, and perform

Extensive simulations to demonstrate theefficiency of our scheme in terms of storage andcomputation overhead

The remainder of this paper is organized as follows: Section2 overviews the related work. In Section3, somepreliminaries and cryptographic primitives are reviewed. In

Section 4, we describe the system model and our designgoals. In Section 5, the proposed scheme is presented indetail, followed by the security analysis and the performanceanalysis in Sections 6 and 7. Finally, we conclude thepaper in Section 8.

2. LITERATURE SURVEY

In [4], Kallahalla et al. proposed a cryptographic storage system that enables secure file sharing on untrusted servers,named Plutus. By dividing files into filegroups and encryptingeach filegroup with a unique file-block key, the dataowner can share the filegroups with others through deliveringthe corresponding lockbox key, where the lockbox key isused to encrypt the file-block keys. However, it brings abouta heavy key distribution overhead for large-scale file sharing.Additionally, the file-block key needs to be updated anddistributed again for a user revocation. Undesired effort, restoration of blur image is very important in many of the cases [3].

In [5], files stored on the untrusted server include twoparts: file metadata and file data. The file metadata impliesthe access control information including a series ofencrypted key blocks, each of which is encrypted underthe public key of authorized users. Thus, the size of the filemetadata is proportional to the number of authorized users.The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadataneeds to be updated. In their extension version, the NNLconstruction [10] is used for efficient key revocation.However, when a new user joins the group, the privatekey of each user in an NNL system needs to be recomputed,which may limit the application for dynamic groups.Another concern is that the computation overhead ofencryption linearly increases with the sharing scale.

Ateniese et al. [6] leveraged proxy reencryptions tosecure distributed storage. Specifically, the data ownerencrypts blocks of content with unique and symmetriccontent keys, which are further encrypted under a masterpublic key. For access control, the server uses proxycryptography to directly reencrypt the appropriate contentkey(s) from the master public key to a granted user's publickey. Unfortunately, a collusion attack between the untrustedserver and any revoked malicious user can belaunched, which enables them to learn the decryption keysof all the encrypted blocks.

In [3], Yu et al. presented a scalable and fine-grained dataaccess control scheme in cloud computing based on the KPABEtechnique. The data owner uses a random key toencrypt a file, where the random key is further encryptedwith a set of attributes using KP-ABE. Then, the groupmanager assigns an access structure and the correspondingsecret key to authorized users, such that a user can onlydecrypt a ciphertext if and only if the data file attributessatisfy the access structure. To achieve user revocation, themanager delegates tasks of data file reencryption and usersecret key update to cloud servers. However, the single-attorneymanner may hinder the implementation of applicationswith the scenario, where any member in a groupshould be allowed to store and share data files with others.

Lu et al. [7] proposed a secure provenance scheme,which is built upon group signatures and ciphertext-policyattribute-based encryption techniques. Particularly, thesystem in their scheme is set with a single attribute. Eachuser obtains two keys after the registration: a groupsignature key and an attribute key. Thus, any user is ableto encrypt a data file using attribute-based encryption andothers in the group can decrypt the encrypted data usingtheir attribute keys. Meanwhile, the user signs encrypteddata with her group signature key for privacy preservingand traceability. However, user revocation is not supportedin their scheme.

From the above analysis, we can observe that how tosecurely share data files in a multiple-owner manner fordynamic groups while preserving identity privacy from anuntrusted

cloud remains to be a challenging issue. In thispaper, we propose a novel Mona protocol for secure datasharing in cloud computing. Compared with the existingworks, Mona offers unique features as follows:

1. Any user in the group can store and share data files with others by the cloud.

2. The encryption complexity and size of ciphertextsare independent with the number of revoked usersin the system.

3. User revocation can be achieved without updating the private keys of the remaining users.

4. A new user can directly decrypt the files stored inthe cloud before his participation.

3. PRELIMINARIES

3.1 Bilinear Maps

Let G_1 and G_2 be an additive cyclic group and a multiplicative cyclic group of the same prime order q, respectively [11]. Let e : $G_1 \times G_1 \rightarrow G_2$denote a bilinear map constructed with the following properties:

1. Bilinear: for all a,bЄZq* and P,QЄG1,e(aP,bQ)=e(P,Q)^{ab}

2. Nondegenerate: There exists a point P such thatE(P,P)≠1.

3. Computable: There is an efficient algorithm tocompute e(P,Q) for any P,QЄG_1

3.2 Complexity Assumptions

Definition 1 (q-strong Diffie-Hellman (q-SDH) Assumption[12]). Given (P_1,P2, γ P_2, γ2P2 ,…. γq qP_2),it is infeasible to compute 1\γ + x

Definition 2 (Decision linear (DL) Assumption [12]). GivenP1,P2, P3,aP1, bP2, cP3, it is infeasible to decide whether a+b=c mod q.

Definition 3 (Weak Bilinear Diffie-Hellman Exponent(WBDHE) Assumption [13]). For unknown a Zq* , given

Y,aY,a^{2}Y ; ::; a^{1}Y ,PЄ G1, it is infeasible to compute e(Y,P)$^{1\a}$

Definition 4 ((t,n)-general Diffie-Hellman Exponent

(GDHE) Assumption [14]). Let f(X)= π $^r_{i=1}$ (X + x_i) and g(X)=π$^{n-r}_{i=1}$ (X+x_i) be two random univariate polynomials. For unknown k, γЄ Zq*,givenG_0, γ G_0,… , γt − 1G_0,γf(γ),G_0,P_0,kg(γ)H_0ЄG_1 and e(G_0, H_0)$^{f2(}$γ$^{)g(}$γ)ЄG_2.It is infeasible to compute e(G_0, H_0)$^{f2(}$γ$^{)g(}$γ)ЄG_2.

3.3 Group Signature

The concept of group signatures was first introduced in [15]

by Chaum and van Heyst. In general, a group signaturescheme allows any member of the group to sign messageswhile keeping the identity secret from verifiers. Besides, thedesignated group manager can reveal the identity of thesignature's originator when a dispute occurs, which isdenoted as traceability. In this paper, a variant of the shortgroup signature scheme [12] will be used to achieveanonymous access control, as it supports efficient membershiprevocation.

3.4 Dynamic Broadcast Encryption

Broadcast encryption [16] enables a broadcaster totransmit encrypted data to a set of users so that only aprivileged subset of users can decrypt the data. Besidesthe above characteristics, dynamic broadcast encryptionalso allows the group manager to dynamically includenew members while preserving previously computed information, i.e., user decryption keys need not be recomputed, the morphology and size of ciphertexts are unchanged and the group encryption key requires no modification. The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique in [14], which will be used as the basis for file sharing in dynamic groups.

4. EXISTING SYSTEM

In the literature study we have many methods for secure data sharing in cloud computing, however most methods failed to achieve the efficient as well as secure method for data sharing for groups. To provide the best solutions for the problems imposed by existing methods, recently the new method was MONA[1].this approach presents the design of secure data sharing scheme, Mona for dynamic groups in an untrusted cloud. InMona, a user is able to share data with the others in the group without revealing identity privacy to the cloud. Additional Mona supports efficient user revocation and new user joining. Morespecially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users and new users can directly decrypt files stored in the cloud before their participation

Disadvantage

1.However as per reliability and scalability concern this method needs to be workout further as if the group manager stop working due to large number of requests coming from different groups of owners, then entire security system fail down.

2.Secure environments protect their resources against unauthorized access by enforcing access control mechanism when increasing is an issue of text based password are not counter for such problems, using instant messaging service is available in the Internet user will obtain one time password(OTP)

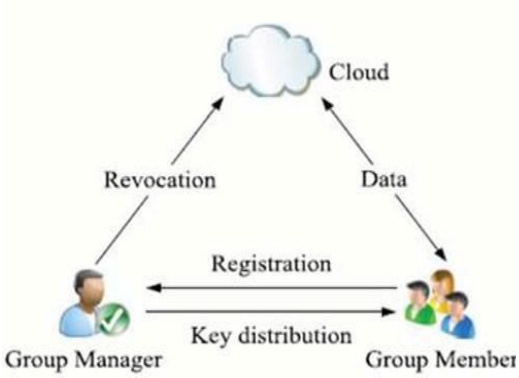

FIGURE1 EXISTING SYSTEM MODEL

5 SYSTEM MODEL AND DESIGN GOALS

5.1 System Model

To achieve the reliable, scalable and higher level security in MONA, in this method we are further processing how we are managing the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in the case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability and providing higher level security

Backup Group Manager

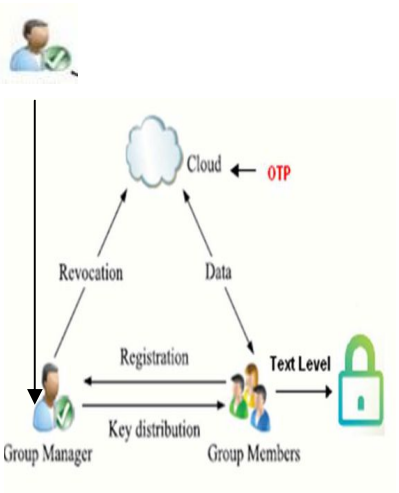

FIGURE2 PROPOSED SYSTEM MODEL

MODEL DESCRIPTION

1. Cloud is operated by CSPs and provides priced abundant storage services. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of thecloud users' trusted domain. Similar to [3], [7], we assume that the cloud server is honest but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes [17], [18], but willtry to learn the content of the stored data and the identitiesof cloud users.

2. GROUP MANAGER

Group manager takes following charges

1. System parameters generation

2. User registration

3. Traceability

4. User revocation

In the givenexample, the group manager is acted by the administratorof the company. Therefore, we assume that the groupmanager is fully trusted by the other parties.

3. Group member

Group members are asset of registered users that will store their private data into the cloud server and share them with others in the group, note that group membership is dynamically changed. Group members can upload the file and download the file within the group.

4. FILE SECURITY

1. Encrypting the data file

2. File stored in the cloud can be deleted by either group manager or the owner of the file

5. GROUP SIGNATURE

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

6. USER REVOCATION

User revocation is performed by the group manager via public available revocation list based on which group members can encrypt their data files and confidentiality against the revoked users.

5.2 DESIGN GOALS

Reliability: it can be achieved by using a backup group manager.

Higher level security: it can be achieved by using instantmessaging service is available in the Internet user will obtain one time password (OTP)

Access control: The requirement of access control is twofold.First, group members are able to use the cloud

resource fordata operations. Second, unauthorized users cannot accessthe cloud resource at any time, and revoked users will beincapable of using the cloud again once they are revoked.

Data confidentiality: Data confidentiality requires thatunauthorized users including the cloud are incapable oflearning the content of the stored data. An important andchallenging issue for data confidentiality is to maintain itsavailability for dynamic groups. Specifically, new usersshould decrypt the data stored in the cloud before theirparticipation, and revoked users are unable to decrypt thedata moved into the cloud after the revocation.

Anonymity and traceability: Anonymity guarantees thatgroup members can access the cloud without revealing the real identity. Although anonymity represents an effectiveprotection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attackermay store and share a mendacious information to derivesubstantial benefit. Thus, to tackle the inside attack, thegroup manager should have the ability to reveal the realidentities of data owners.

Efficiency: The efficiency is defined as follows: Any groupmember can store and share data files with others in thegroup by the cloud. User revocation can be achievedwithout involving the remaining users. That is, theremaining users do not need to update their private keys or reencryption operations. New granted users can learn allthe content data files stored before his participation withoutcontacting with the data owner.

6. PROPOSED SCHEMA

6.1 Overview

To achieve secure data sharing for dynamic groups in thecloud, we expect to combine the group signature anddynamic broadcast encryption techniques. Specially, thegroup signature scheme enables users to anonymously use

the cloud resources, and the dynamic broadcast encryption

technique allows data owners to securely share their data

files with others including new joining users.Unfortunately, each user has to compute revocationparameters to protect the confidentiality from the revokedusers in the dynamic broadcast encryption scheme, whichresults in that both the computation overhead of theencryption and the size of the ciphertext increase with thenumber of revoked users. Thus, the heavy overhead andlarge ciphertext size may hinder the adoption of thebroadcast encryption scheme to capacity-limited users.To tackle this challenging issue, we let the groupmanager compute the revocation parameters and makethe result public available by migrating them into the cloud.Such a design can significantly reduce the computationoverhead of users to encrypt files and the ciphertext size. Specially, the computation overhead of users for encryptionoperations and the ciphertext size is constant andindependent of the revocation users.

6.2 SCHEME DESCRIPTION

This section describes the details of Mona including system

initializations, user registration, user revocation, file generation,file deletion, file access and traceability.

6.2.1 System Initialization

The group manager takes charge of system initialization

as follows:Generating a bilinear map group system S=(q,G1,G2,e(.,.)).the system parameters include(S,P,H,H0,H1,H2,U,V,W,Y,Z,f,f1,Enc()), where f is a one way hash function:{0,1}*->Z*q;f1 is hash function:{0,1}*->G1;and Enck() is a secure symmetric encryption algorithm with the secret key k.

6.2.2 User registration

For the registration of user I with identity IDi, the group manager randomly selects a number xi belong to Z*q and computes Ai, Bi as the following equation:

$$\begin{cases} A_i = \dfrac{1}{\gamma + x_i} \cdot P \in G_1 \\ B_i = \dfrac{x_i}{\gamma + x_i} \cdot G \in G_1. \end{cases}$$

Then, the group manager adds (Ai, xi, IDi) into thegroup user list, which will be used in the traceability phase.

After the registration, user i obtains a private key (xi, Ai, Bi) which will be used for group signature generationand file decryption

6.2.3 Revocation list

User revocation is performed by the group manager via apublic available revocation list (RL), based on which group

members can encrypt their data files and ensure theconfidentiality against the revoked users.

Table 1 revocation list

IDgroup	D1	y1	t1	P1		
	D2	y2	t2	P2		
	.	.	.	.		
	Dr	yr	tr	Pr	Wr	tRL sig(RL)

the revocation list is characterized by a series oftime stamps t1,t2,…tr. In the proposed system once the user time stamp over does not wait for the group manager to update the time stamp or revocation list here once the time over the userimmediately send request for extra time for access the data to the cloud. Then the cloud will send that request to the group manager once the see it and give permission then the cloud will time to access the data but if the group manager did not give permission then the cloud will not give permission for access if the data

6.2.4 File generation

To store and share a data file in the cloud, a group member performs the following operations: Getting the revocation list from the cloud . In this step, the member sends the group identity IDgroup as a request to the cloud. Then, the cloud responds the revocation list RL to the member. Verifying the validity of the received revocation list. First, checking whether the marked date is fresh. Second, verifying the contained signature sig(RL) by the equation e(W, f1 (RL)) = e(P, sig(RL)). If the revocation list is invalid, the data owner stops this scheme. Encrypting the data file M. Selecting a random number T and computing fT. The hash value will be used for data file deletion operation. In addition, the data owner adds (IDdata, T) into his local storage. Constructing the uploaded data file as shown in Table 2, where tdata denotes the current time on the member, and a group signature on (IDdata, C1, C2, C, f(T); tdata) computed by the data owner through private key (A, x).

Table 2: Message Format

Group ID	Data ID	ciphertext	hash	Time	Signature
ID_{group}	ID_{data}	C_1, C_2, C	$f(\tau)$	t_{data}	σ

Uploading the data shown in Table 2 into the cloud server and adding the IDdata into the local shared data list maintained by the manager. On receiving the data, the cloud first check its validity. If the algorithm returns true, the group signature is valid; otherwise, the cloud abandons the data. In addition, if several users have been revoked by the group manager, the cloud also performs revocation verification. Finally, the data file will be stored in the cloud after successful group signature and revocation verifications.

6.2.5 File deletion

The file stored in the cloud can be deleted by either the group manager or the data owner .To delete a file IDdata , the group manager computes a signature and sends the signature along with IDdata to the cloud.

7 PERFORMANCE EVALUTAION

7.1 Storage

Without loss of generality, we set q=160 and the elements

in G1 and G2 to be 161 and 1,024 bit, respectively. In addition, we assume the size of the data identity is 16 bits, which yield a group capacity of 216 data files. Similarly, the size of user and group identity are also set as 16 bits.

Group manager. In Mona, the master private key of the

group manager is $(G,\gamma,\varepsilon1,\varepsilon2)\epsilon G1\times Z^{q}_{3}$.Additionally,

the user list and the shared data list should be stored at the

group manager. Considering an actual system with 200 usersand assuming that each user share 50 files in average, thetotal storage of the group manager is $(80.125+42.125*200+2*10{,}000)*10^{-3} \approx 28.5$ kbytes,which is very acceptable.

Group members. Essentially, each user in our scheme only

needs to store its private key $(A_i, B_i, x_i)$is about 60 bytes. It is worth noting that there is a tradeoffbetween the storage and the computation overhead. For example, the four pairing operations including $(e(H,W),e(H,P),e(P,P),e(A_i,P))\epsilon G^{4}_{2}$can be precomputedonce and stored for the group signature generation andverification. Therefore, the total storage of each users isabout 572 bytes.

The extra storage overhead in the cloud. In Mona, the format

of files stored in the cloud is shown in Table 2. Since C3 is theciphertext of the file under the symmetrical encryption, theextra storage overhead to store the file is about 248 bytes,which includes $(ID_{group}, ID_{data}, C1, C2, C3, f(\tau), d_{ata}, \sigma)$.

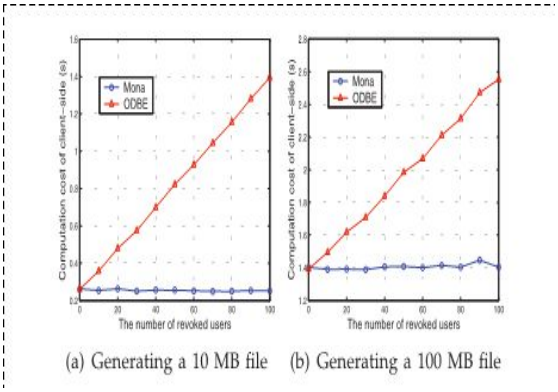

Figure 3 comparison on computation cost for file generation between Mona and ODBE [14]

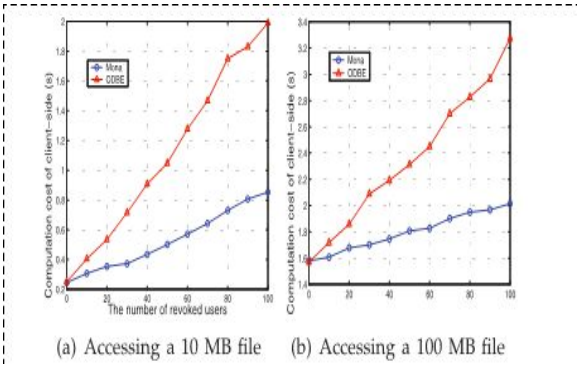

Figure 4 comparison on computation cost for the file access between Mona and ODBE [14]

7.2 Simulation

The simulation consists of threecomponents:clientside, manager side as well as cloud side. Both client side and manager side process are conducted on laptop with core 2T7250 2.0Ghz processor,DDR2 800 2G,ubuntu 10.04X86.The cloud side process is implemented on machine that equipped with core 2 i3-2350 2.3 GHz,DDR3 1066 2G,Ubuntu 12.04X64.In the simulation ,we choose an elliptic curve with 160 bit group order ,which provides a competitive security level with 1024bit RSA.

7.2.1 Client Computation Cost

In Fig. 3, we list the comparison on computation cost ofclients for data generation operations between Mona and theway that directly using the original dynamic broadcastencryption (ODBE) [14]. It is easily observed that thecomputation cost in Mona is irrelevant to the number ofrevoked users. On the contrary, the computation costincreases with the number of revoked users in ODBE. Thereason is that the parameters $(P_r Z_r)$ can be obtained from the revocation list without sacrificing the security in Mona,while several time-consuming operations including pointmultiplications in G1 and exponentiations in G2 have to be performed by clients to compute the parameters in ODBE.

From Figs. 3a and 3b, we can find out that sharing a 10 Mbytefile and a 100-Mbyte one, cost a client about 0.2 and 1.4 seconds in our scheme, respectively, this implies that the symmetrical encryption operation domains the computationcost when the file is large.

The computation cost of clients for file access operation with the size of 10 and 100 Mbytes are illustrated in Fig. 4.

The computation cost in Mona increases with the number of revoked users, as clients require to perform Algorithms 3 and 4 to compute the parameter Ar,r and check whether the data owner is a revoked user. Besides the above operations, P1, P2, Pr needs to be computed by clients in ODBE.Therefore, Mona is still superior to ODBE in terms ofcomputation cost. Similar to the data generation operation,the total computation cost is mainly determined by thesymmetrical decryption operation if the accessed file is large, which can be verified from Figs. 4a and 4b. In addition, the file deletion for clients is about 0.075 seconds, because it only costs a group signature on a message (IDdata,τ)where _ is a 160-bit number in Zq^*.

7.2.2 Cloud Computation Cost

To evaluate the performance of the cloud in Mona, we testits computation cost to respond various client operationrequests including file generation, file access, and filedeletion. Assuming the sizes of requested files are 100 and 10 MB, the test results are given in Table 3. It can be seen thatthe computation cost of the cloud is deemed acceptable,even when the number of revoked users is large. This isbecause the cloud only involves group signature andrevocation verifications to ensure the validity of therequestor for all operations. In addition, it is worth noting that the computation cost is independent with the size of the requested file for access and deletion operations, since the size of signed message is constant.

Table 3 computation cost of the cloud (s)

Request	The number of revoked users		
	0	50	100
File generation (100 MB)	0.065	0.154	0.271
File generation (10 MB)	0.045	0.125	0.226
File access (100 MB)	0.045	0.150	0.237
File access (10 MB)	0.045	0.151	0.240
File deletion (100 MB)	0.041	0.153	0.240
File deletion (10 MB)	0.042	0.156	0.238

8 CONCLUSION

In this paper we design a secure data sharing scheme for dynamic groups,also achieve an scalability more importantly reliability and providing higher level security using one time password(OTP). Additionally, this technique supports efficient user revocation and new user joining.More specially, efficient

user revocation can be achievedthrough a public revocation list without updating theprivate keys of the remaining users, and new users candirectly decrypt files stored in the cloud before theirparticipation. Moreover, the storage overhead and theencryption computation cost are constant. Extensive analysesshow that our proposed scheme satisfies the desiredsecurity requirements and guarantees efficiency as well.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-attorney Data Sharing for Dynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131- 145, 2003.

[5] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[6] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[8] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001. [12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[13] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[14] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[15] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[16] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[17] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Intl Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[18] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[19] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Query in Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, pp. 46- 50, 2008.

[20] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532, 2001

